UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/799,455	03/12/2004	Sean E. Purcell	MS308121.1/MSFTP644US	7697

27195 7590 02/20/2008

AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
MAI, KEVIN S	

ART UNIT	PAPER NUMBER
4121	

NOTIFICATION DATE	DELIVERY MODE
02/20/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
osteuball@thepatentattorneys.com

Office Action Summary	Application No.	Applicant(s)	
	10/799,455	PURCELL ET AL.	
	Examiner	Art Unit	
	KEVIN S. MAI	4121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/14/2004, 11/12/2004, 1/19/2005, 3/31/2005, 10/28/2005, 1/20/2006, 2/27/2006, 3/21/2006, 5/10/2006, 7/31/2006, 11/7/2006, 11/29/2006, 2/7/2007, 3/19/2007, 5/10/2007, 8/23/2007, 11/29/2007, 1/16/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 40 have been examined and are pending.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 40 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. A data packet is seen to be non-statutory subject matter since it is the same as claiming program code. As such the data packet as disclosed appears to be non-statutory subject matter.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 – 9, 18 – 28, 34 and 38 – 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pub. No. 2005/0165895 to Rajan et al. (hereinafter "Rajan") and further in view of U.S. Pub. No. 2005/0097174 to Daniell et al. (hereinafter "Daniell").

As to Claim 1, Rajan teaches **a system that mitigates viewing offensive message content comprising:**

a message receiving component that receives at least one incoming message for delivery to a user (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale. Where taking in incoming mail is seen to inherently suggest the existence of a message receiving component)**;**

a filtering component that calculates a junk score for the message (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages)**; and**

Rajan does not teach but Daniell teaches **a content blocking component that blocks at least a portion of message content from appearing in at least a preview pane when the junk score exceeds a first threshold** (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature of displaying a preview of a selected message has been disabled. This is because the message has been determined to be objectionable or undesired. This is seen to be the same as the claimed limitation because the portion being blocked is the entire message and since the message is in the spam folder it is apparent that the message has exceeded some threshold of for spam detection).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine calculating a junk score for incoming messages as taught by Rajan, with blocking a message from appearing in the preview pane as taught by Daniell. One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to prevent unintentional viewing of content determined to be objectionable or undesired. Since the purpose of a spam filtering is to prevent the user from viewing content they do not wish to view, it would be obvious to prevent the user from seeing the content via the preview pane until it was explicitly accessed. "Common sense teaches, however, that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle...When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense." See KSR v. Teleflex, 550 U.S. ___, 127 S. Ct. 1727 (2007).

As to Claim 2, Rajan and Daniell teach **the system of claim 1, further comprising a classification component that classifies the message as any one of good, junk, and a middle state** (Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30

would be left in the inbox. This is seen to be the same as having a good, junk, and middle state) **for messages determined to be safe for an inbox but not safe for viewing or previewing the message based in part on the junk score** (Paragraph [0032] of Rajan discloses that some email may be placed in more than one directory such as the inbox (white) directory and the gray directory. Then in paragraph [0043] of Daniell it is disclosed that the feature of displaying a preview of a selected message can be disabled for spam messages. Thus it is seen that those that are rated gray/white would be in the inbox but since it is spam would still have the preview disabled).

Examiner recites the same rationale to combine used in Claim 1.

As to Claim 3, Rajan and Daniell teach **the system of claim 2, the message is classified at least in the middle state when the junk score exceeds at least the first threshold** (Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox. Thus it is seen that exceeding the first threshold of 30 in this situation would be classifying a message in the middle state).

As to Claim 4, Rajan and Daniell teach **the system of claim 1, further comprising an analysis component that determines whether the junk score exceeds the first threshold** (Paragraph [0016] of Rajan discloses an example of a spam scale

from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox. This classification step is seen to imply that determination of a message exceeding a threshold is done by the system).

As to Claim 5, Rajan and Daniell teach **the system of claim 1, further comprising an unblocking component that receives user input to unblock blocked message content** (Paragraph [0043] of Daniell discloses that messages in the spam folder may be viewed by using the message center to select a message from the spam folder and then selecting the read button. This allows the user to read the text associated with the selected message. Since the message that was in the spam folder was previously not viewable in the preview screen (blocked) and then distinct user input (selecting the read button) allows the letter to be read (unblocked), this is seen to be the same as the claimed limitation).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as taught by Rajan and Daniell, with having the ability to unblock as taught by Daniell.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to complete the functionality of the spam filter. Spam filters always risk the chance of blocking content that the user actually wishes to view. Thus it would be convenient to be able to unblock the blocked content so that the user

could use an unmark as spam button to move a message to the inbox (paragraph [0044] of Daniell)

As to Claim 6, Rajan and Daniell teach **the system of claim 5, the unblocking component operates per message** (Paragraph [0043] of Daniell discloses that messages in the spam folder may be viewed by using the message center to select a message from the spam folder and then selecting the read button. This is applying only to the selected message and as such is operating per message)**.**

Examiner recites the same rationale to combine used in Claim 5.

As to Claim 7, Rajan and Daniell teach **the system of claim 1, the content blocking component operates per message or globally for substantially all messages** (Paragraph [0032] of Rajan discloses that some email may be placed in more than one directory such as the inbox (white) directory and the gray directory. Then in paragraph [0043] of Daniell it is disclosed that the feature of displaying a preview of a selected message can be disabled for spam messages. Thus it is seen that those that are rated gray/white would be in the inbox but since it is spam would still have the preview disabled. This scenario represents blocking operating per message. However in paragraph [0043] of Daniell the preview window being disabled applies to the whole spam folder, this implies the ability to disable the preview window for specific folders. If

all folders were then disabled it would be the same as the blocking component operating globally).

Examiner recites the same rationale to combine used in Claim 1.

As to Claim 8, Rajan and Daniell teach **the system of claim 1, the content comprises text, links, sounds, video, attachments, embedded content, applets, speech, and images** (These are seen to be obvious things to expect in an e-mail. Thus since the claimed invention deals with the content in e-mail it would be obvious to expect content to comprise the items above).

"Common sense teaches, however, that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle...When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense." See KSR v. Teleflex, 550 U.S. ___, 127 S. Ct. 1727 (2007).

As to Claim 9, Rajan and Daniell teach **the system of claim 1, the first threshold determined in part by user preferences** (Paragraph [0031] of Rajan

discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges. These ranges are seen to be the same as the thresholds).

As to Claim 18, Rajan and Daniell teach **the system of claim 1, further comprising a rating component that rates incoming messages as unscanned before they are subjected to the filtering component** (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded).

As to Claim 19, Rajan and Daniell teach **the system of claim 18, unscanned messages are hidden from view and are not visible in a user's inbox while additional data about the message is collected or while the message is being filtered by the filtering component** (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded. Since they are not placed into the inbox until after filtering, the messages are effectively hidden from view and are not visible).

As to Claim 20, Rajan and Daniell teach **the system of claim 18, unscanned messages are made visible in a user's inbox when the filtering component is turned off** (Figure 4 of Daniell discloses being able to turn off spam filtering and next to the selection it is explained that all emails will be delivered to the inbox. Thus it is seen that when filtering is off all messages would be visible)**.**

It is seen that being able to turn off the filter is an obvious feature of the system. Furthermore, once the filter it turned off it is taught in Daniell that all emails will be delivered to the inbox. Given that nothing will be marked as spam, none of them would be blocked and as such they would all be visible. Thus it is seen that this limitation is taught by Rajan and Daniell.

"Common sense teaches, however, that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle...When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense." See KSR v. Teleflex, 550 U.S. ___, 127 S. Ct. 1727 (2007).

As to Claim 21, Rajan and Daniell teach **a computer readable medium having stored thereon the system of claim 1** (Claim 11 of Rajan discloses a computer-readable medium comprising program instructions for its invention).

As to Claim 22, Rajan teaches **a method that mitigates viewing offensive message content comprising:**

receiving at least one incoming message (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale);

computing a junk score for the at least one message (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages); **and**

Rajan does not teach but Daniell teaches **blocking at least a portion of message content from appearing in at least a preview pane when the junk score exceeds a blocking threshold** (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature of displaying a preview of a selected message has been disabled. This is because the message has been determined to be objectionable or undesired. This is seen to be the same as the claimed limitation because the portion being blocked is the entire message

and since the message is in the spam folder it is apparent that the message has exceeded some threshold of for spam detection).

Examiner recites the same rationale to combine used in Claim 1.

As to Claim 23, Rajan and Daniell teach **the method of claim 22, further comprising classifying the message based in part on a computed junk score** (Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox).

As to Claim 24, Rajan and Daniell teach **the method of claim 22, filer comprising classifying the message as unscanned before computing the junk score** (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded).

As to Claim 25, Rajan and Daniell teach **the method of claim 24, further comprising updating the message from unscanned to some other rating based in part on its computed junk score** (Paragraph [0030] of Rajan discloses as incoming e-

mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded. However after being graded it is then moved to the appropriate directories at which point it would be classified under those directories. Thus the score is seen to be updated).

As to Claim 26, Rajan and Daniell teach **the method of claim 22, the content comprising at least one of text, images, sounds, audio, video, applets, embedded text, embedded images, URLs, and speech** (These are seen to be obvious things to expect in an e-mail. Thus since the claimed invention deals with the content in e-mail it would be obvious to expect content to comprise the items above).

"Common sense teaches, however, that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle...When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense." See KSR v. Teleflex, 550 U.S. ___, 127 S. Ct. 1727 (2007).

As to Claim 27, Rajan and Daniell teach **the method of claim 22, further comprising unblocking blocked content when explicit user input to unblock the content is received** (Paragraph [0043] of Daniell discloses that messages in the spam folder may be viewed by using the message center to select a message from the spam folder and then selecting the read button. This allows the user to read the text associated with the selected message. Since the message that was in the spam folder was previously not viewable in the preview screen (blocked) and then distinct user input (selecting the read button) allows the letter to be read (unblocked), this is seen to be the same as the claimed limitation).

Examiner recites the same rationale to combine used in Claim 5.

As to Claim 28, Rajan and Daniell teach **the method of claim 22, blocking the message content applies to substantially all messages globally when feature is activated** (Paragraph [0043] of Daniell the preview window being disabled applies to the whole spam folder, this implies the ability to disable the preview window for specific folders. If all folders were then disabled it would be the same as the blocking component operating globally).

Examiner recites the same rationale to combine used in Claim 1.

As to Claim 34, Rajan teaches **a system that mitigates viewing offensive message content comprising:**

means for receiving at least one incoming message (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale)**;**

means for computing a junk score for the at least one message (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages)**; and**

Rajan does not teach but Daniell teaches **means for blocking at least a portion of message content from appearing in at least a preview pane when the junk score exceeds a blocking threshold** (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature of displaying a preview of a selected message has been disabled. This is because the message has been determined to be objectionable or undesired. This is seen to be the same as the claimed limitation because the portion being blocked is the entire message and since the message is in the spam folder it is apparent that the message has exceeded some threshold of for spam detection)**.**

Examiner recites the same rationale to combine used in Claim 1.

As to Claim 38, Rajan and Daniell teach **the system of claim 34, further comprising means for unblocking blocked content when explicit user input to unblock the content is received** (Paragraph [0043] of Daniell discloses that messages in the spam folder may be viewed by using the message center to select a message from the spam folder and then selecting the read button. This allows the user to read the text associated with the selected message. Since the message that was in the spam folder was previously not viewable in the preview screen (blocked) and then distinct user input (selecting the read button) allows the letter to be read (unblocked), this is seen to be the same as the claimed limitation).

Examiner recites the same rationale to combine used in Claim 5.

As to Claim 39, Rajan and Daniell teach **the system of claim 34, further comprising means for classifying the message as unscanned before computing the junk score** (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded).

As to Claim 40, Rajan teaches **a data packet adapted to be transmitted between two or more computer processes that mitigates viewing offensive message content, the data packet comprising** (Paragraph [0031] of Rajan discloses that the system may employ a server/client topology where the information may be processed by either individually or partly by both. Thus since they need to communicate it would be seen that a data packet exists that comprised the following information)**: information associated with receiving at least one incoming message** (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale)**; computing a junk score for the at least one message** (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages)**.** Rajan does not teach but Daniell teaches **blocking at least a portion of message content from appearing in at least a preview pane when the junk score exceeds a blocking threshold** (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature of displaying a preview of a selected message has been disabled. This is because the message has been determined to be objectionable or undesired. This is seen to be the same as the claimed limitation because the portion being blocked is the entire message and since the message is in the spam folder it is apparent that the message has exceeded some threshold of for spam detection)**.**

Examiner recites the same rationale to combine used in Claim 1.

5. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rajan and Daniell as applied to claim 1 above, and further in view of U.S. Pub. No. 2002/0147782 to Dimitrova et al. (hereinafter "Dimitrova").

As to Claim 10, Rajan and Daniell teach **the system of claim 1.** Rajan and Daniell do not teach but Dimitrova teaches **the content blocking component blocks at least a portion of the message content by performing at least one of the following:**

hiding at least a portion of the content of the message;

hiding at least a portion of a subject line of the message;

hiding content in a from line of the message;

blurring at least a portion of the subject line of the message;

blurring content in the from line of the message; and

blurring at least a portion of the content of the message (Paragraph [0016] of Dimitrova discloses masking portions of the video or audio content, for example blurring a naked body. It is noted that Dimitrova suggests in paragraph [0035] implementing the parental control system in an e-mail system. Thus it is seen that Dimitrova teaches performing at least one of the above actions).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as taught by Rajan and Daniell, with blurring content as taught by Dimitrova.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to permit a method of parental control that filter only the offending portions instead of merely blocking entire messages (Paragraph [0012] of Dimitrova). This would allow a child to view the majority of a message, but not content a parent would deem unfit for the child to view.

6. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rajan and Daniell as applied to claim 1 above, and further in view of U.S. Pub. No. 2003/0009495 to Adjaoute (hereinafter "Adjaoute").

As to Claim 11, Rajane and Daniell teach **the system of claim 1.** Rajan and Daniell do not teach but Adjaoute teaches **the content blocking component replaces blocked content with at least one of text, graphics, video, and/or audio notice that warns users that potentially offensive content has been blocked from view** (Paragraph [0057] of Adjaoute discloses that if the content is restricted, then a message is displayed instead of the content saying that the access to the content has been restricted. It is noted that Adjaoute deals primarily with websites however in paragraph [0029] it suggest the software plug-in being installed in an email application).
It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as taught by Rajan and Daniell, with replacing the blocked content as taught by Adjaoute.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to help the filter prevent viewing of offensive material. Paragraph [0006] of Adjaoute shares that the goal would be to control the information that children can receive. Thus it is seen that it would be advantageous to block the material and inform the participant that what they are trying to access has been blocked.

7. Claims 12 – 17, 30 – 33, 35 and 36 – 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rajan and Daniell as applied to claims 1, 22, and 34 above, and further in view of U.S. Pub. No. 2003/0204569 to Andrews et al. (hereinafter "Andrews").

As to Claim 12, Rajan and Daniell teach **the system of claim 1.** Rajan and Daniell do not teach but Andrews teaches **further comprising a challenge-response component that requests message senders to correctly respond to at least one challenge per message received when the junk score of that message exceeds a second threshold before delivery of the message is permitted** (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as taught by Rajan and Daniell, with the challenge system taught by Andrews.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to increase the security of the spam filter. Andrews explains in paragraph [0007] that a challenge would help verify that the source of the potentially infected/spam email is a human and not a machine. Since most spam is generated by a machine as opposed to individually sent out by humans such a system would help filter out many messages.

As to Claim 13, Rajan, Daniell and Andrews teach **the system of claim 12, the second threshold is any one of higher or lower than the first threshold** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges. It is noted that because Rajan teaches a user setting up the configurations for his various spam directories that it would be obvious to either have the second threshold higher or lower depending on the personal preference of the user).

As to Claim 14, Rajan, Daniell and Andrews teach **the system of claim 12, the second threshold is about equal to the first threshold** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges.

Since the ranges are determined by the user, making the second threshold about equal to the first would be easily done).

As to Claim 15, Rajan, Daniell and Andrews teach **the system of claim 12, the second threshold is determined at least in part by user preferences** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges. These ranges are seen to be the same as the thresholds).

As to Claim 16, Rajan, Daniell and Andrews teach **the system of claim 12, the message associated with the challenged sender is hidden from view in a user's inbox until the challenge is correctly solved** (Figure 1 of Andrews discloses a letter being detained in the smart email filtering system until a correct response is received. This is effectively hiding the message from view until it is correctly solved).

Examiner recites the same rationale to combine used in claim 12.

As to Claim 17, Rajan, Daniell and Andrews teach **the system of claim 12, content of the message is blocked when the message is released to the user's inbox following a correctly solved challenge since the message's junk score exceeds the first threshold** (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a

message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things, the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox. It is seen that since the letter was placed into the inbox and that, as taught above, letters in the inbox with sufficient ratings are blocked, it would be obvious that after a message comes back from a challenge that it would still be blocked once deposited in the inbox).

Examiner recites the same rationale to combine used in claim 12.

As to Claim 30, Rajan and Daniell teach **the method of claim 22.** Rajan and Daniell do not teach but Andrews teaches **further comprising challenging a sender of the message before revealing any blocked content of the message** (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things, the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox).

Examiner recites the same rationale to combine used in claim 12.

As to Claim 31, Rajan and Daniell teach **the method of claim 22.** Rajan and Daniell do not teach but Andrews teaches **further comprising challenging a sender of the message before allowing delivery of the message when the junk score of the message exceeds a challenge threshold** (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things, the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox).

As to Claim 32, Rajan, Daniell and Andrews teach **the method of claim 31, the challenge threshold is any one of higher or lower than the blocking threshold** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges. It is noted that because Rajan teaches a user setting up the configurations for his various spam directories that it would be obvious to either have the second threshold higher or lower depending on the personal preference of the user).

As to Claim 33, Rajan, Daniell and Andrews teach **the method of claim 31, the challenge threshold is about equal to the blocking threshold** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective

ranges. Since the ranges are determined by the user, making the second threshold about equal to the first would be easily done).

As to Claim 35, Rajan and Daniell teach **the system of claim 34.** Rajan and Daniell do not teach but Andrews teaches **further comprising means for challenging a sender of the message before allowing delivery of the message when the junk score of the message exceeds a challenge threshold** (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things, the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox).

Examiner recites the same rationale to combine used in claim 12.

As to Claim 36, Rajan, Daniell and Andrews teach **the system of claim 35, the challenge threshold is any one of higher or lower than the blocking threshold** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges. It is noted that because Rajan teaches a user setting up the

configurations for his various spam directories that it would be obvious to either have the second threshold higher or lower depending on the personal preference of the user).

As to Claim 37, Rajan, Daniell and Andrews teach **the system of claim 35, the challenge threshold is about equal to the blocking threshold** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges. Since the ranges are determined by the user, making the second threshold about equal to the first would be easily done).

8. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rajan and Daniell as applied to claim 22 above, and further in view of U.S. Pub. No. 2005/0080889 to Malik et al. (hereinafter "Malik").

As to Claim 29, Rajan and Daniell teach **the method of claim 22.** Rajan and Daniell do not teach but Malik teaches **further comprising requiring a password to open messages in which content has been blocked** (Paragraph [0071] of Malik discloses child protection in an email system where it can be set such that to get access to a child's spam folder one would have to enter in the master or parent password. This is seen to be the same as needing a password to access messages that are blocked).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of claim 22 as taught by Rajan and Daniell, with requiring a password as taught by Malik.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to prevent children from viewing content that a parent would deem inappropriate for viewing. Thus it is to provide a method that restricts a child type user from performing a restricted operation (paragraph [0007] Malik).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- U.S. Pub. No. 2005/0050150 "Filter, System and Method for Filtering an Electronic Mail Message" to Dinkin

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KEVIN S. MAI whose telephone number is (571)270-5001. The examiner can normally be reached on Monday through Friday 7:30 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KSM

/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 4121
2/11/2008